CRYPTO-CURRENCY

LA CRITTOGRAFIA E LA BLOCKCHAIN

LA BOLLA

ethereum

PANORAMICA

Prev. Chiudi
922.4078

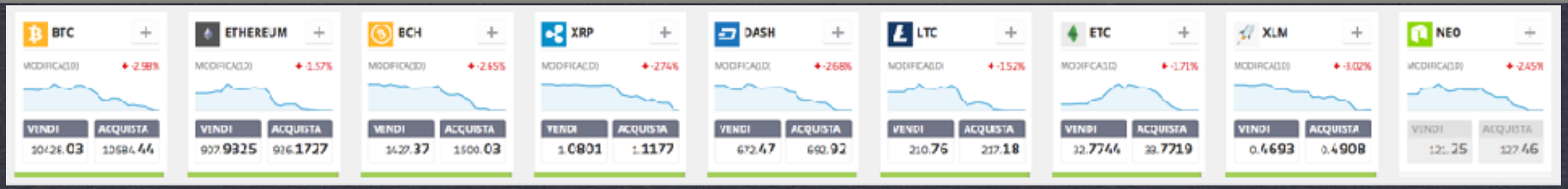
Variazione Giornali...
919.9130 - 926.1908

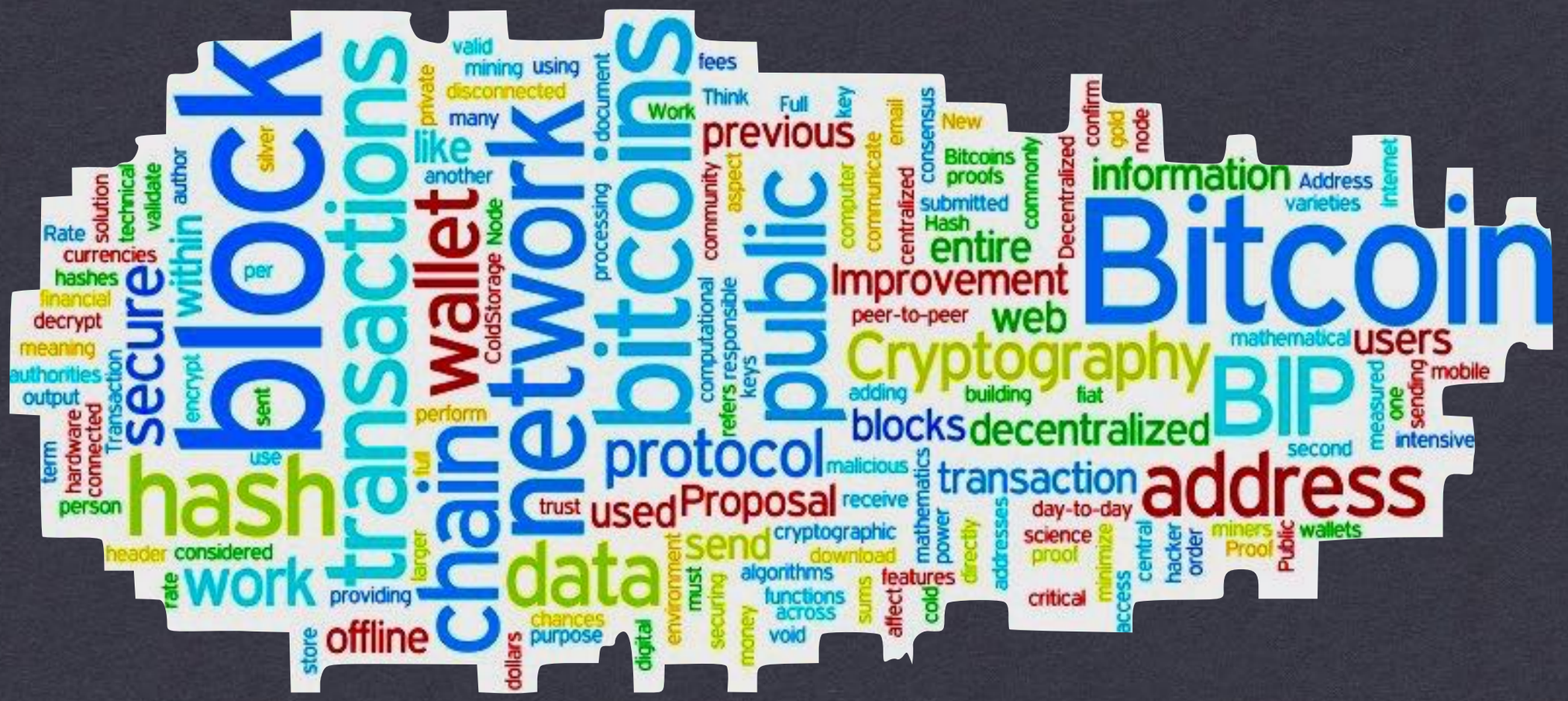
Variazione 52 Sett.
12.1300 - 1412.8503

Rendimento a 1 anno
7,218.95%

Orari dei grafici in UTC

https://www.etoro.com/it/discover/markets/cryptocurrencies



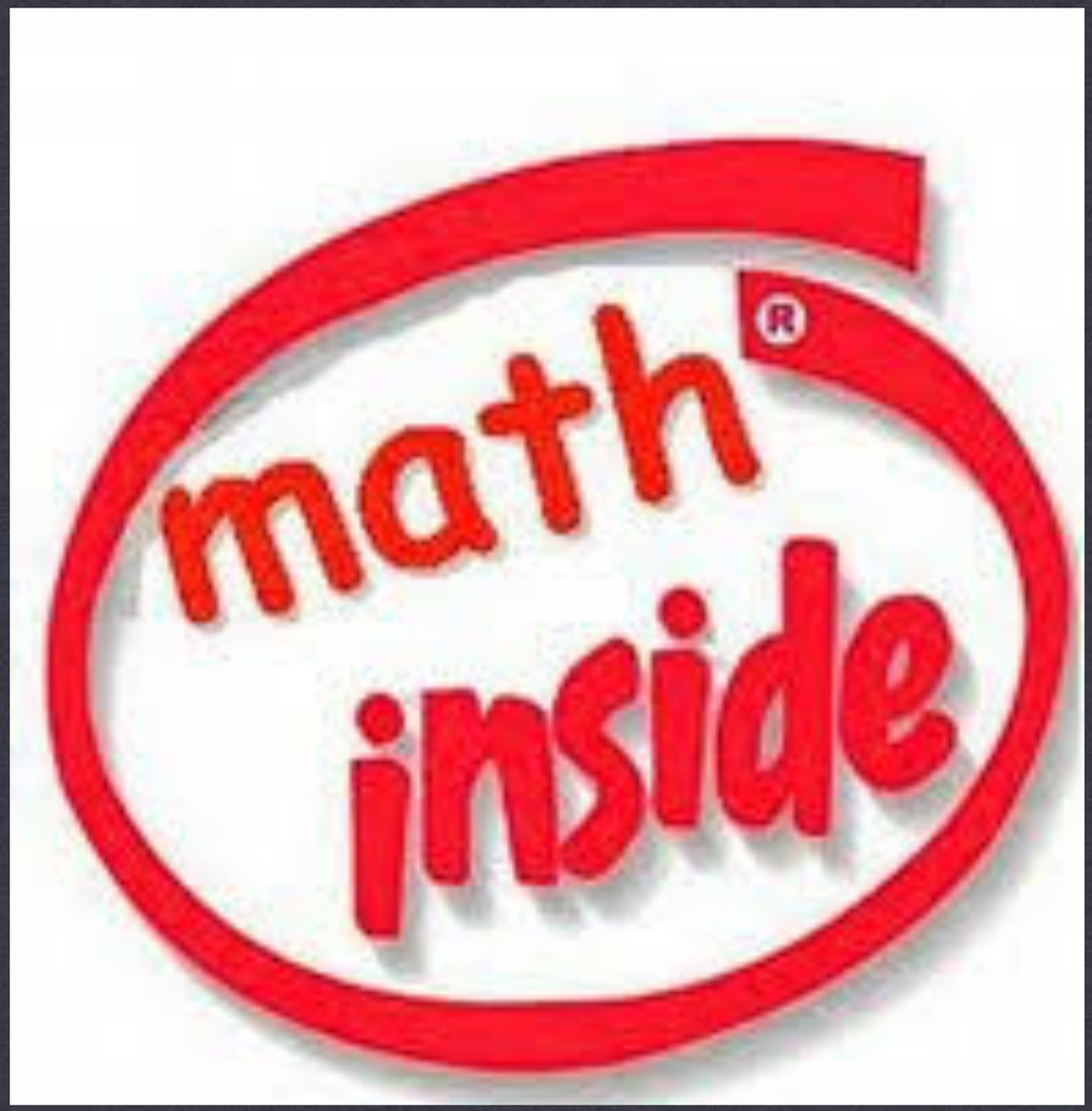


LE MONETE VIRTUALI

FRA TRADING E VIRTÙ

PERCHÉ CRYPTO

ALGEBRA, PROBABILITÀ E COMPLESSITÀ COMPUTAZIONALE SONO ALL'OPERA PER GARANTIRE LA SICUREZZA DI QUESTE MONETE VIRTUALI



TRE

I FONDAMENTI CRITTOGRAFICI

non falsificabili

l'emissione di nuova moneta è un processo crittografico, non manipolabile.

non alterabili

gli scambi di moneta vengono registrati e una volta avvenuti non possono essere modificati.

tracciabili

l'origine di ogni trasferimento è univocamente identificata, non è possibile ripudiare una transazione.

A=10 EUR

A -> B 2 EUR

B -> C 1 EUR

A -> C 2 EUR

LA TECNOLOGIA

LE CRYPTO-MONETE METTONO IN PRATICA IL CONCETTO PIÙ GENERALE DI BLOCKCHAIN.

la sequenza di transazioni viene registrata pubblicamente in modo che movimenti effettuati siano non modificabili e non ripudiabili. Inoltre non c'è un'entità che centralizza la registrazione delle informazioni.

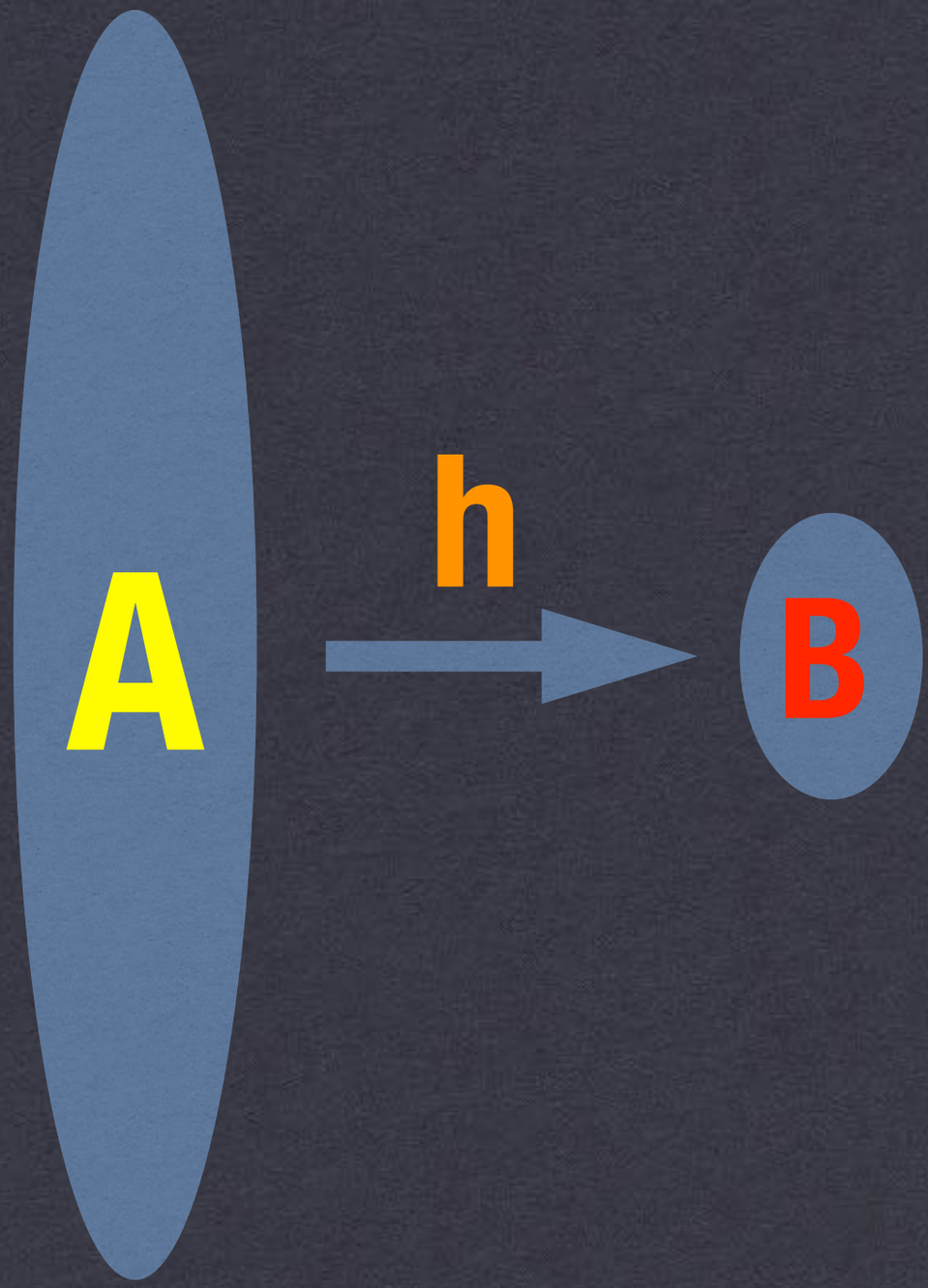
HASH FUNCTIONS

LE FUNZIONI DI HASH (DALL'INGLESE TO HASH: SMINUZZARE, PASTICCIARE) IN INFORMATICA SI INTENDE UNA FUNZIONE (ESPRESSA DA UNA FORMULA MATEMATICA O DA UN ALGORITMO) CHE PERMETTE DI OTTENERE DA UNA SEQUENZA DI BIT DI **LUNGHEZZA ARBITRARIA** UNA SEQUENZA DI BIT DI **LUNGHEZZA PREDEFINITA**.

73de30c0c6e60fdd4b2d69189d94aff2

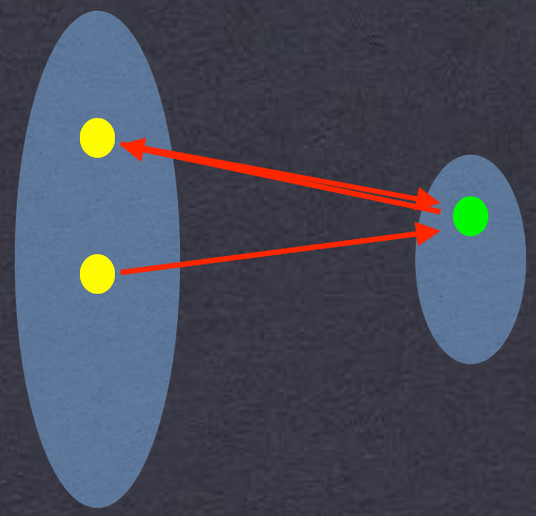
FUNZIONI NON INVERTIBILI

PER MOTIVI DI SPAZIO CI SARANNO MOLTI (INFINITI) ELEMENTI DI A CHE PRODUCONO LO STESSO HASH IN B MA QUANDO SONO CRITTOGRAFICHE LE HASH FUNCTIONS SONO FATTE IN MODO CHE CAMBIANDO ANCHE DI UN SOLO BIT LA SEQUENZA DI INPUT SI OTTIENE UN VALORE MOLTO DIVERSO



HASH FUNCTIONS SICURE

LE PROPRIETÀ RICHIESTE AD UNA HASH FUNCTION SICURA SONO MISURATE DALLA DIFFICOLTÀ DI TROVARE SOLUZIONE AI SEGUENTI PROBLEMI (LEGATI ALLA NON INVERTIBILITÀ)



- **PROBLEMA DELLA CONTROIMMAGINE:** DIFFICOLTÀ DI CALCOLARE UNA SEQUENZA CHE ABBIA UN HASH FISSATO
- **PROBLEMA DELLA COLLISIONE:** DIFFICOLTÀ DI CALCOLARE DUE SEQUENZE CON LO STESSO HASH
- **PROBLEMA DELLA SECONDA CONTROIMMAGINE:** DIFFICOLTÀ DI CALCOLARE UNA SEQUENZA CHE ABBIA LO STESSO HASH DI UNA SEQUENZA FISSATA.

CHAINING

A=10 EUR → hash1

A -> B 2 EUR (hash1) → hash2

B -> C 1 EUR (hash2) → hash3

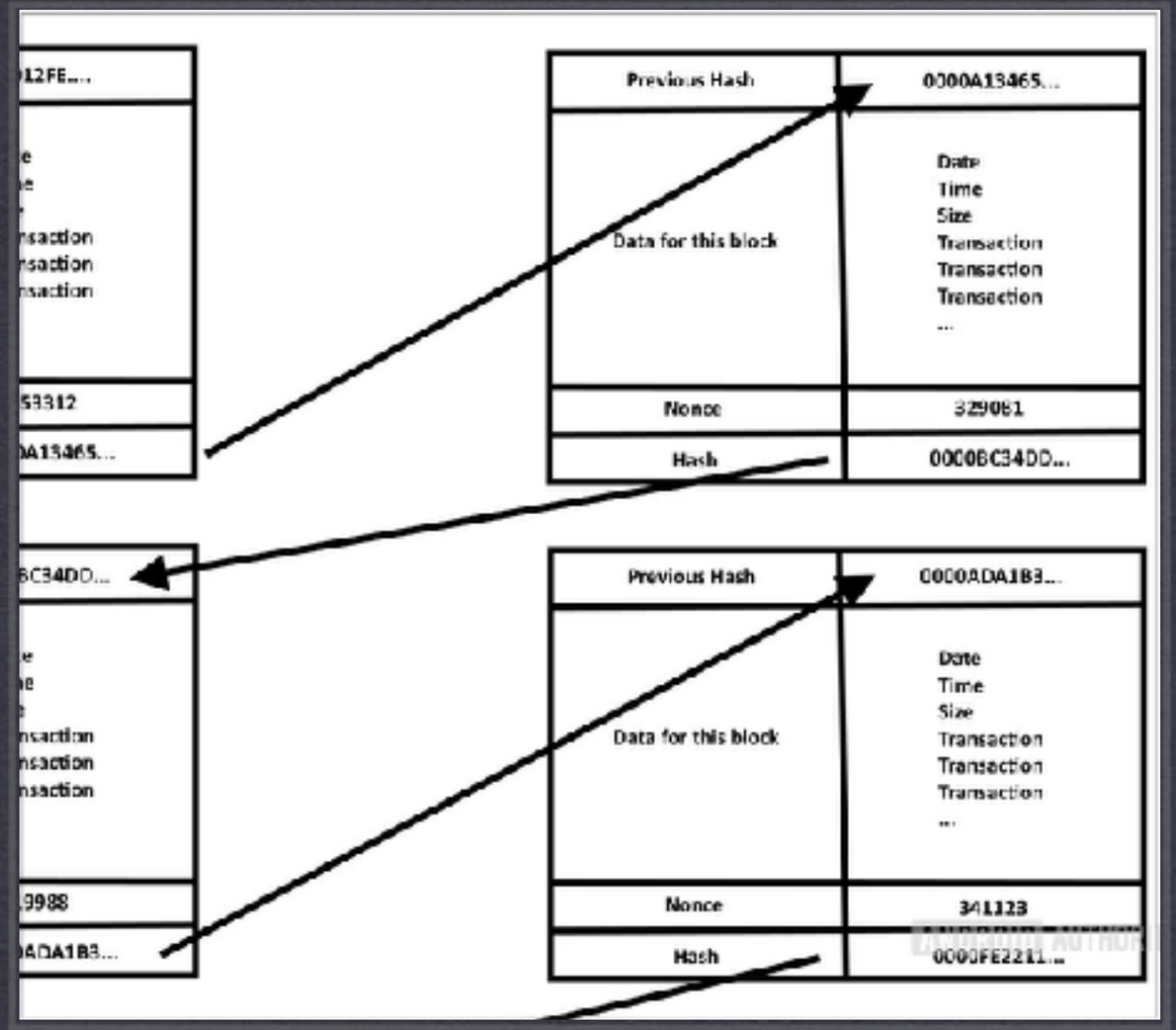
A -> C 2 EUR (hash3) → hash4

UNA FUNZIONE DI HASH FORNISCE UNA FIRMA (PRATICAMENTE) UNIVOCA E QUINDI NON FALSIFICABILE.

Una funzione di hash associa ad ogni elemento appartenente ad uno spazio di dimensioni enormi un elemento di uno spazio piccolo (l'hash); in modo tale che la probabilità di trovare un elemento con un dato hash sia molto bassa.

NON ALTERABILE

UNA VOLTA CHE UNA TRANSAZIONE È STATA INSERITA NELLA **CHAIN** QUESTA NON PUÒ ESSERE PIÙ MODIFICATA SENZA INVALIDARE TUTTO IL RESTO DELLA CATENA.



LE TRANSAZIONI VENGONO RAGGRUPPATE IN BLOCCHI E OGNI CIRCA 10 MINUTI UN NUOVO BLOCCO DI TRANSAZIONI VIENE EMESSO DIVENENDO PARTE DEL REGISTRO DI TRANSAZIONI (IL LOG FILE) CHE VIENE COMUNEMENTE DENOMINATO BLOCKCHAIN; IL FATTO CHE UNA TRANSAZIONE FACCIA PARTE DELLA BLOCKCHAIN LA RENDE UFFICIALE (O SAREBBE MEGLIO DIRE UFFICIALIZZABILE).

TRANSAZIONI E I BLOCCHI

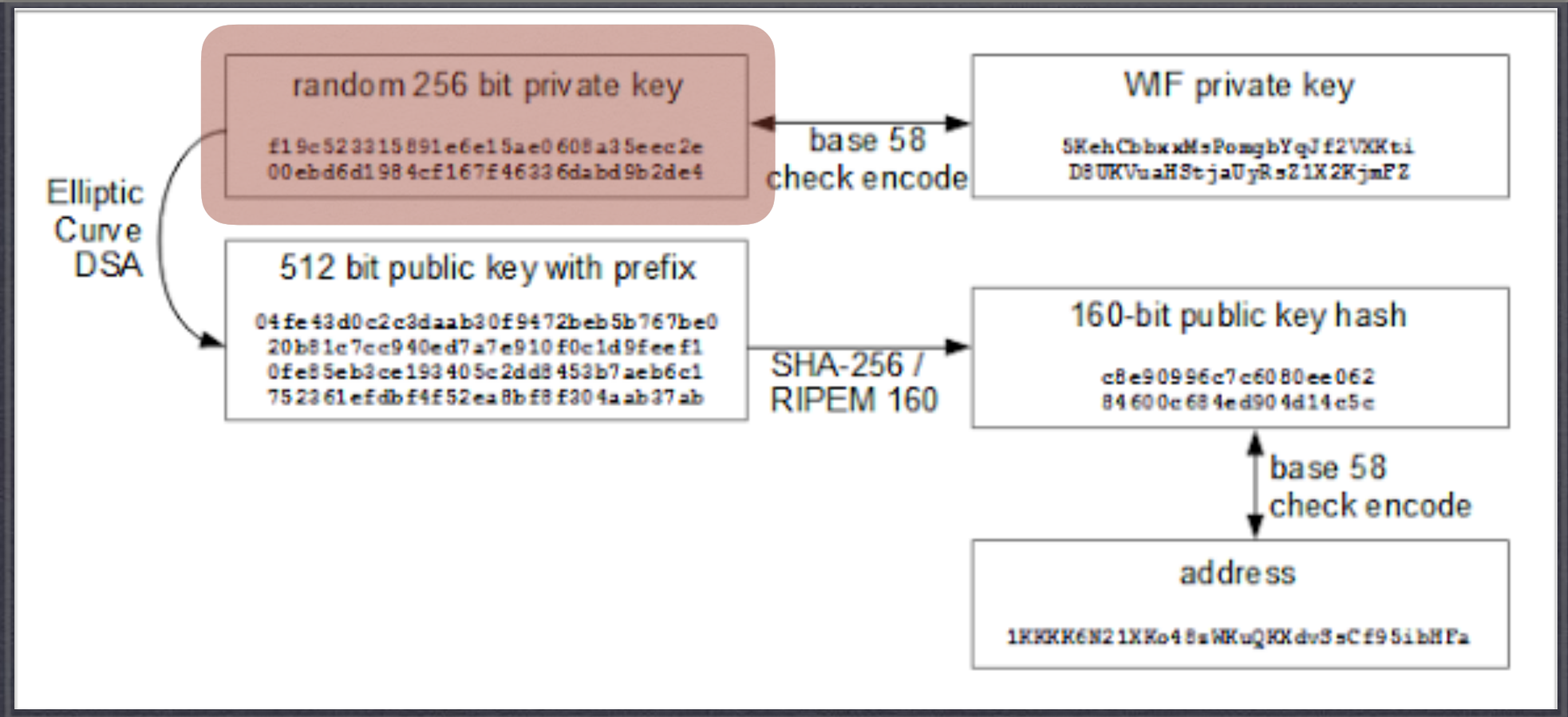
UNA TRANSAZIONE (NEL CASO DELLE CRYPTO-MONETE) CONSISTE IN UN PASSAGGIO DI UNA CERTA QUANTITÀ DI VALUTA DA UN PORTAFOGLIO AD UN ALTRO, LE TRANSAZIONI VENGONO RAGGRUPPATE IN BLOCCHI ED I BLOCCHI CONCATENATI AL REGISTRO DEL SISTEMA

A -> B 2 EUR

- A indica il portafoglio dell'utente che deve cedere della valuta
- B indica il portafoglio verso cui bisogna inviare la valuta.

Nel caso dei BITCOIN la valuta appartiene ad un **indirizzo bitcoin**, quindi A e B saranno le entità coinvolte nella transazione e avranno identificatori del tipo:

`1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa`



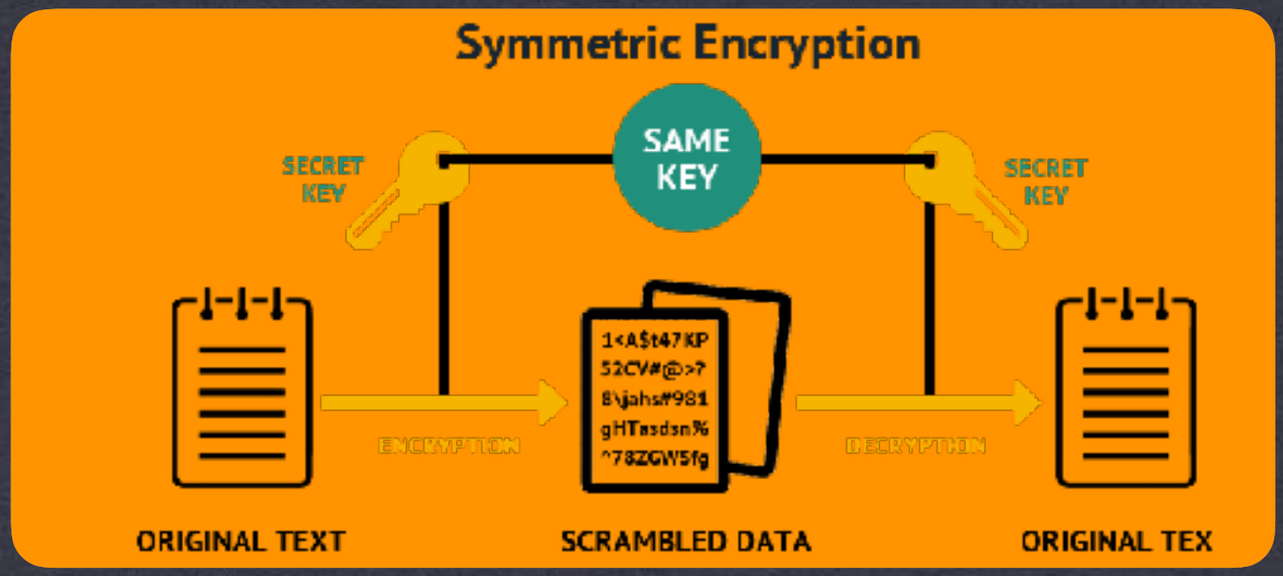
L'INDIRIZZO

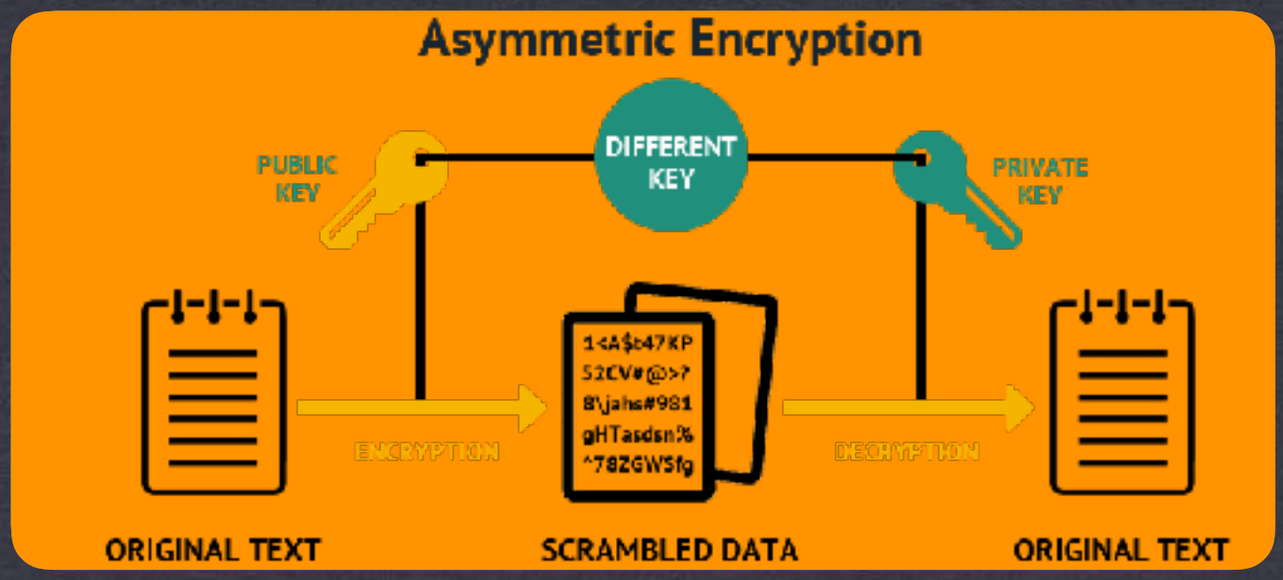
UN INDIRIZZO BITCOIN IDENTIFICA IL PORTAFOGLIO CHE CONTIENE LE MONETE, ED È L'HASH DELLA PARTE PUBBLICA DI UNA COPPIA DI CHIAVI PER LA CIFRATURA ASIMMETRICA SECONDO LO SCHEMA A CURVE ELLITTICHE ECDSA

- **WIF = WALLET IMPORT FORMAT è la codifica ASCII della sequenza di bit data dalla chiave privata che è scelta casualmente.**
- **L'indirizzo serve come identificatore del possessore di bitcoin ed è una codifica dell'hash della chiave pubblica.**

CRITTOGRAFIA ASIMMETRICA

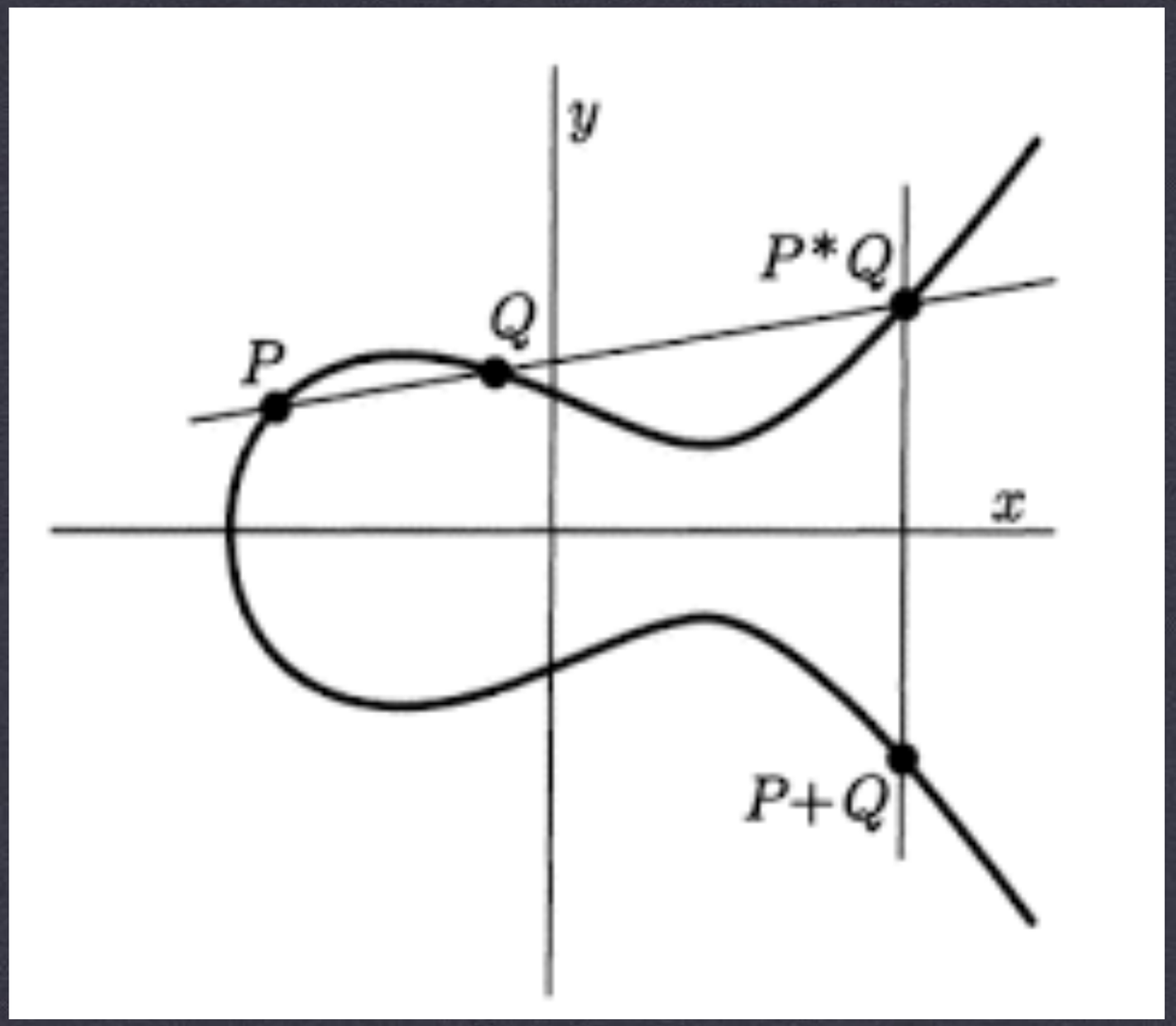
NELLA CRITTOGRAFIA A CHIAVE PUBBLICA SI UTILIZZANO COPPIE DI CHIAVI (PUB,PRIV) IN MODO CHE LE DUE PARTI CHE DEVONO APPLICARE LO SCHEMA CRITTOGRAFICO NON DEBBANO CONCORDARE PREVENTIVAMENTE UNA CHIAVE COMUNE





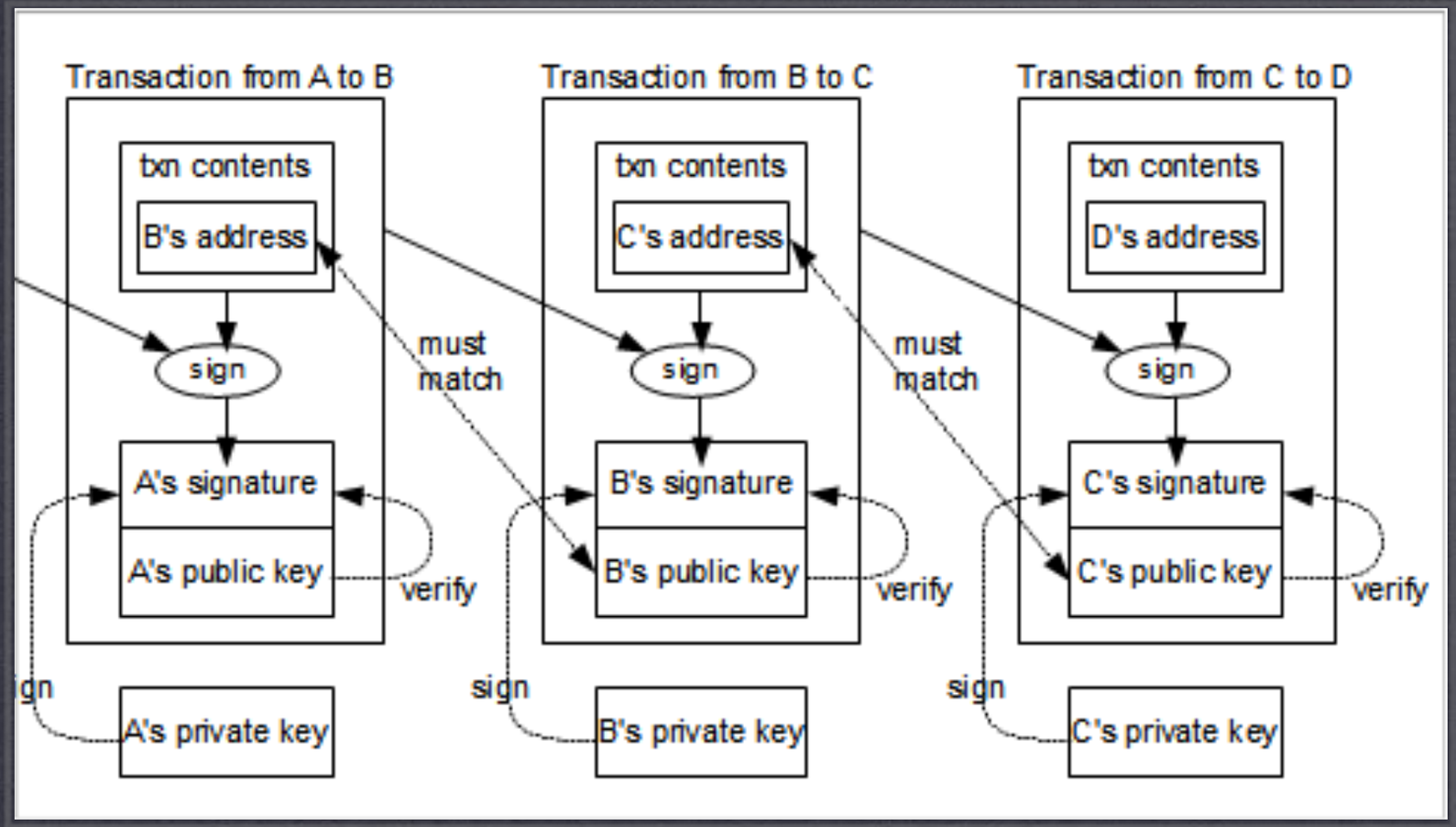
CURVE ELLITTICHE

SI FISSA UNA CURVA, E SI CONSIDERA L'OPERAZIONE TRA PUNTI DELLA CURVA DEFINTA GEOMETRICAMENTE



IL LOGARITMO DISCRETO: CONSISTE NEL RISOLVERE L'EQUAZIONE **x P = Q** dove x è un numero intero metre P e Q sono punti dati della curva. DAL PUNTO DI VISTA COMPUTAZIONALE LA SOLUZIONE DI QUESTA EQUAZIONE è UN COMPITO DIFFICILE. x corrisponde alla chiave privata, mentre il punto Q corrisponde alla chiave pubblica.

ECDSA



HASHING

LA CHIAVE PUBBLICA PERMETTE DI CREARE CON LA CHIAVE PRIVATA DEGLI HASH CHE POSSONO ESSERE VERIFICATE AVENDO ACCESSO SOLO ALLA CHIAVE PUBBLICA

Un utente A può generare una transazione su un certo portafgolio solo se possiede la chiave privata corrispondente all'indirizzo del portafoglio. In realtà non c'è un posto dove le monete si accumulano ma la quantità di monete corrispondenti ad un certo portafoglio si trova nella blockchain (come risultato delle transazioni). I bitcoin possono essere gestiti dal possessore della chiave privata corrispondente.

MINING

IL BITCOIN MINING CONSISTE NEL PROCESSO CHE INSERISCE LA TRANSAZIONE NELLA BLOCKCHAIN, L'OPERAZIONE CHE CREA UNA VISIONE CONSISTENTE E CONDIVISA DEL REGISTRO DELLE TRANSAZIONI.

PER SCAVARE UN BLOCCO (BLOCK MINING), BISOGNA TROVARE UNA SOLUZIONE MOLTO RARA DI UN PROBLEMA DI CRITTOGRAFIA.

L'archivio dei blocchi non è gestito in modo centralizzato per cui si possono creare situazioni di conflitto, per questo i blocchi vengono proposti per l'inserimento e solo dopo una validazione (in cui si risolvono le situazioni di conflitto) il blocco viene inserito.

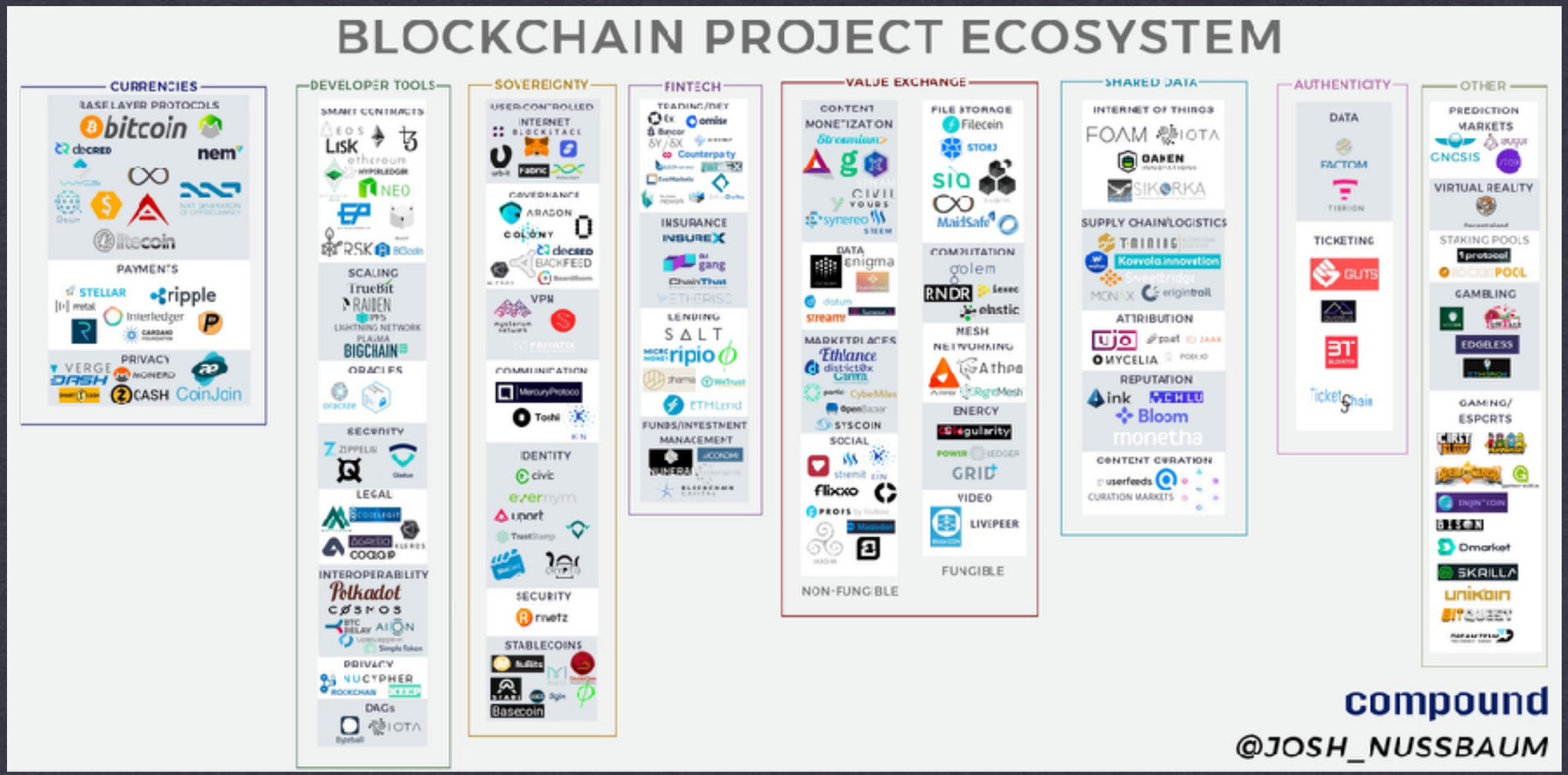
LA RETE PEER-TO-PEER

IL BLOCCO DA VALIDARE VIENE INSERITO NELLA RETE CHE P2P CHE GESTISCE L'ARCHIVIO DELLE TRANSAZIONI, E VIENE "MINED" OVVERO SI CERCA L'HASH CHE SODDISFA LA CONDIZIONE FISSATA. CHI FA QUESTO LAVORO ? PERCHÉ ?

Il mining corrisponde al coniare moneta.

Molti computer vengono costruiti per effettuare questo compito, sono macchine speciali adattate per effettuare l'hashing velocemente consumando poca elettricità. Chi risolve il problema e valida un blocco riceve un premio in bitcoin, pertanto diventa un modo di guadagnare (in crypto-valuta, convertibile sui siti di cambio).

LA BLOCKCHAIN NON SI LIMITA ALLE CRYPTO-MONETE MA FA PARTE DI UN PROGETTO PIU' AMPIO CHE COINVOLGE MOLTI CAMPI DI INTERESSE.



GRAZIE !